On sums and differences of powers of rational numbers

Luis H. Gallardo and Philippe Goutet

Abstract

Given two nonzero integers $a, b \in \mathbb{Z}^*$, we characterize the rational numbers x, y such that $ax^n - by^n \in \mathbb{Z}$ for all non-negative integers $n \in \mathbb{N}$.

1 Introduction

If a rational number $x \in \mathbb{Q}$ has a power which is an integer, then x itself is forced to be an integer by the fundamental theorem of arithmetic. In other words if we have $x = \frac{N}{D}$ with a positive integer D and an integer N, and both satisfy $(N/D)^r = K$ (where K is an integer), for some positive integer r, where N/D is a reduced fraction (N and D have no common factors, we also say that N and D are *coprime*); then by comparing exponents of each prime number appearing in both sides of the equality

$$N^r = D^r K$$

we get $D = 1$ so that $x = N$ is indeed an integer.

A natural generalization of this problem consists in looking at $c_n = ax^n - by^n$ where a, $b \in \mathbb{Z}^*$ are two nonzero integers and x, $y \in \mathbb{Q}$ are two rational numbers, and asking if the existence of some values of n such that c_n is an integer, i.e., $c_n \in \mathbb{Z}$ implies that x and y are indeed integers, i.e., x, $y \in \mathbb{Z}$.

The existence of only one n such that $c_n \in \mathbb{Z}$ is not sufficient, as shown, for example (check it !), by the relation $(\frac{13}{2})^5 + (\frac{19}{2})^5 = 88981 \in \mathbb{Z}$. However, the result becomes true with the stronger assumption that all the c_n are in $\mathbb{Z}$.

Theorem 1 *Consider two nonzero integers $a, b \in \mathbb{Z}^*$ and two rational numbers $x, y \in \mathbb{Q}$. If, for all $n \in \mathbb{N}$, $ax^n - by^n \in \mathbb{Z}$, then x and y are both integers unless $a = b$ and $x = y$.*

Robert Israel (University of British Columbia), gives a direct proof [3] of the case $a = b = 1$. At the end of the present note, we look at how to weaken the assumption that *all* the c_n are in $\mathbb{Z}$ when $a \neq b$.

We recall some classical notation used in the proof: If a and b are two integers such that there exists an integer m such that $ma = b$ then we say that a divides b and we write: $a \mid b$. As usual, we write $d = \gcd(a, b)$ their greatest common divisor, so that, for example, $\gcd(17, 51) = 17$, while $\gcd(a, b) = 1$ is equivalent to a, b are coprime. Now, we fix a positive integer $n \in \mathbb{N}$. First of all, Euler's totient function computed on n, denoted $\varphi(n)$ gives us the number of positive integers h in between 1 and n that are coprime with n. Second, and this is a little more complicated object we consider here: the n-th cyclotomic polynomial $\Phi_n(t)$ is a one variable polynomial in the indeterminate t with integral coefficients that has the property that it is the polynomial, with integer coefficients, of minimal degree that vanishes when $t = w$ where the complex, but non-real, number $w \in \mathbb{C}$ is a n-th root of unity; this means that $w^n = 1$. For example, $\Phi_3(t) = t^2 + t + 1$, since $\Phi_3(t) = \frac{t^3-1}{t-1}$ shows that $\Phi_3(w) = 0$ for $w = \frac{-1+i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}$ and also for $w^2 = \frac{-1-i\sqrt{3}}{2} = e^{\frac{-2\pi i}{3}}$, where w, w^2 are the, non-real, 3-roots of unity in the field of complex numbers $\mathbb{C}$; while any polynomial of degree 1 with integer coefficients cannot vanish simultaneously in w and in w^2. A nice result of Gauss is that the degree of $\Phi_n(t)$ is precisely $\varphi(n)$.

2 The proof

We write x and y as irreducible fractions $x = \frac{N}{D}$ and $y = \frac{M}{E}$ with $D, E > 0$. In order to show that both x and y are integers, we proceed in two steps, first showing that $D = E$ and then showing that $D = 1$.

Lemma 1 *$D = E$.*

Proof. As $c_n = ax^n - by^n \in \mathbb{Z}$, we have $aN^nE^n - bM^nD^n = c_nE^nD^n$. Since D and N are coprime, we deduce that $D^n \mid aE^n$. Similarly, $E^n \mid bD^n$.

Consider a prime number p and write $a = p^\alpha a'$, $b = p^\beta b'$, $D = p^d D'$, and $E = p^e E'$ with a', b', D', and E' coprime to p. Because $E^n \mid bD^n$, we have $ne \le nd + \beta$ and, similarly, $D^n \mid aE^n$ gives $nd \le ne + \alpha$. By taking $n > \max(\alpha, \beta)$, we deduce that $e \le d$ and $d \le e$ and so $d = e$. As this is valid for any prime p, we conclude that $D = E$.

Lemma 2 *$D = 1$.*

Proof. As $D = E$, we can rewrite $ax^n - by^n = c_n$ as $aN^n - bM^n = c_nD^n$ and so $D^n \mid aN^n - bM^n$ for all $n \in \mathbb{N}$. We consider two cases, depending on whether $a = b$ or not.

First case: $a \neq b$. We have $D^n \mid aN^n - bM^n$ and $D^n \mid D^{2n} \mid aN^{2n} - bM^{2n}$. Hence, $D^n \mid (aN^n - bM^n)(aN^n + bM^n) = a^2N^{2n} - b^2M^{2n}$ and thus $D^n \mid (a^2N^{2n} - b^2M^{2n}) - a(aN^{2n} - bM^{2n}) = b(a-b)M^{2n}$. Because $D = E$ and M are coprime, we deduce that $D^n \mid b(a-b)$. The number $b(a-b)$ is $\neq 0$ because $b \neq 0$ and $a \neq b$, hence $D = 1$.

Second case: $a = b$. This case is a bit more difficult. As mentioned in the Theorem, we exclude the case $x = y$ or else $c_n = 0 \in \mathbb{Z}$ for all n, independently of the value of x. Let $R = \gcd(M, N)$ and write $N = RN_1$ and $M = RM_1$. Because D is coprime to both N and M, D is coprime to R. As $D^n \mid a(N^n - M^n)$, we deduce that $D^n \mid a(N_1^n - M_1^n)$ and we write $a(N_1^n - M_1^n) = a(N_1 - M_1)C_n$ where $C_n = (N_1^n - M_1^n)/(N_1 - M_1)$. Since $D \mid a(N_1 - M_1)$, we deduce, for each n such that C_n is coprime to a and $N_1 - M_1$, that $D^n \mid a(N_1 - M_1)$. If this is true for infinitely many n, we will have $D = 1$ as $a(N_1 - M_1) \neq 0$ since $a \neq 0$ and $x \neq y$.

We are thus reduced to showing that C_n is coprime to both a and N_1-M_1 for infinitely many n. We do so for n a prime number which divides neither N_1-M_1 nor a nor $\varphi(a)$. For such an n, Lemma 3 below applies to show that N_1-M_1 and C_n are coprime and Lemma 5 applies to show that a and C_n are coprime, hence the result.

3 Auxiliary lemmas

We recall the notion of *order* of an integer n modulo a prime number p, say $o_p(n)$: it is the minimal positive integer r such that $n^r \equiv 1 \pmod p$. One knows that $o_p(n)$ divides $\varphi(p)=p-1$; for example (check it !) $o_{1093}(2)=364$.

In the previous proof, we have used the following lemmas. The first two are classical results, but we recall their proofs for the convenience of the reader.

Lemma 3 *Consider $n \geq 1$. If N_1 and M_1 are two coprime integers such that n and N_1-M_1 are coprime, then N_1-M_1 and $C_n=(N_1^n-M_1^n)/(N_1-M_1)$ are coprime.*

In fact, one can show [1, Exercise 71, p. 20] that, if $d=\gcd(a,b)$, then

$$\gcd(\frac{a^n-b^n}{a-b}, a-b) = \gcd(nd^{n-1}, a-b).$$

Proof. Let p be a prime number dividing N_1-M_1. As $N_1 \equiv M_1 \mod p$, we have $M_1^i N_1^j \equiv N_1^{i+j} \mod p$ and thus $C_n \equiv nN_1^{n-1} \mod p$. As n and p are coprime and N_1 and p are also coprime (because p divides N_1-M_1 with N_1 coprime to M_1), we deduce that C_n and p are coprime. This is true for each prime p dividing N_1-M_1, thus C_n and N_1-M_1 are coprime.

Lemma 4 *If $n \neq p$ are two prime numbers, then the existence of $x \in \mathbb{Z}$ such that $\Phi_n(x) \equiv 0 \mod p$ implies that $n \mid \varphi(p)=p-1$.*

Although it simplifies the proof, the fact that n is prime is not necessary as long as n and p are coprime; see [2, Theorem 94, p. 164].

Proof. As $\Phi_n(x) \equiv 0 \mod p$, we have $x^n \equiv 1 \mod p$. Because $\Phi_n(1)=n \not\equiv 0 \mod p$, we deduce that $x \not\equiv 1 \mod p$ and so x is of order n as n is prime. Hence, $n \mid \varphi(p)$.

Lemma 5 *Let n be a prime number, N_1 and M_1 two coprime integers and $C_n = (N_1^n-M_1^n)/(N_1-M_1)$. If n is coprime to both a and $\varphi(a)$, then a is coprime to C_n.*

Proof. As n is a prime number, we can write $C_n = M_1^{n-1}\Phi_n(\frac{N_1}{M_1}) = N_1^{n-1}\Phi_n(\frac{M_1}{N_1})$. Let p be a prime number dividing a; as n and a are coprime, so are n and p; similarly, n and $\varphi(p)$ are coprime since $\varphi(p) \mid \varphi(a)$. Because M_1 and N_1 are coprime, one of them, let's say M_1, is not divisible by p. Denote by M_1' the inverse of M_1 mod p so that $C_n \equiv M_1^{n-1}\Phi_n(N_1M_1') \mod p$. Since $M_1 \not\equiv 0 \mod p$ and $\Phi_n(N_1M_1') \not\equiv 0 \mod p$ by Lemma 4, we have $C_n \not\equiv 0 \mod p$. As this is true for every prime dividing a, we deduce that a and C_n are coprime.

4 Strengthening of the theorem

In the previous theorem, it is not necessary to assume that all the c_n are in $\mathbb{Z}$: we only need $c_n \in \mathbb{Z}$ for $1 \leq n \leq N$ with N sufficiently large. How large depends on a and b, as we will now see in the case $a \neq b$. Before that, we introduce the notation $\epsilon(1) = 0$ and, if $m \geq 2$, $\epsilon(m) = \max_{1 \leq i \leq r} \alpha_i$ where $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ is the prime decomposition of m (all the p_i being distinct).

Proposition 1 *Consider $a \neq b$ in $\mathbb{Z}^*$, $x, y \in \mathbb{Q}$, and $N \in \mathbb{N}$. Assume that $N > \epsilon(a)$, $N > \epsilon(b)$ and $N > 2\epsilon(b(a-b))$. If $ax^n - by^n \in \mathbb{Z}$ for $1 \leq n \leq N$, then x and y are both integers.*

Proof. We only need to show that the proofs of Lemma 1 and Lemma 2 stay valid. In the proof of Lemma 1, we need to be able to take $n > \max(\alpha, \beta)$, which is allowed by the conditions $N > \epsilon(a)$ and $N > \epsilon(b)$. In the case $a \neq b$ of Lemma 2, we need $n > \epsilon(b(a-b))$ for the condition $D^n \mid b(a-b)$ to imply that $D = 1$; but as this condition is obtained by considering $D^{2n} \mid aN^{2n} - bM^{2n}$, we need to be able to take $n > 2\epsilon(b(a-b))$, which is allowed by the condition $N > 2\epsilon(b(a-b))$.

Example: If $a = 2$ and $b = 1$, the minimal N satisfying the assumptions of the previous proposition is $N = 2$ since $\epsilon(a) = 1$ and $\epsilon(b) = \epsilon(b(a-b)) = 0$. By considering $(x, y) = (\frac{1}{2}, 3)$, we see that this value of N is optimal.

References

[1] J.-M. De Koninck and A. Mercier, *1001 Problems in Classical Number Theory*, American Mathematical Society, Providence, Rhode Island, 2007.

[2] T. Nagell, *Introduction to Number Theory*, 2nd ed., Chelsea, New York, 1981.

[3] R. Israel, *Difference of like powers of rational numbers*, posted on the Usenet newsgroup `sci.math`, May 16, 2007, available at `http://sci.tech-archive.net/Archive/sci.math/2007-05/msg02738.html`.

Luis H. Gallardo
University Of Brest, Mathematics
6, Av. Le Gorgeu
C.S. 93837
29238 Brest Cedex 3, France.
`Luis.Gallardo@univ-brest.fr`

Philippe Goutet Institut de
Mathématiques de Jussieu, Université
Paris VI, Boîte courier 247
4 place Jussieu
75252 Paris Cedex, France.
`goutet@math.jussieu.fr`